REMARKS

To advance the prosecution and expedite allowance of this application, Applicants have canceled claims 1-7, 18 and 20-28 without prejudice or disclaimer. Applicants reserve the right to pursue the subject matter of these canceled claims in a continuation application.

The specification has been amended to state Applicants' priority claim from the Irish Patent Application No. S98 0458 filed June 15, 1998; Irish Patent Application No. S98 0346 filed May 7, 1998; and Irish Patent Application No. S98 0223 filed March 25, 1998. Certified copies of these priority documents were submitted with parent Application No. 09/235,836.

The Office Action includes a rejection of claims 1-10, 12-16, 18 and 20-28 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Franklin et al. (U.S. Patent No. 5,883,810) in view of Cohen (U.S. Patent No. 6,422,462). This rejection is respectfully traversed.

As noted above, Applicants have canceled claims 1-7, 18 and 20-28 without prejudice or disclaimer, thus rendering moot the rejection of these claims.

In setting forth the rejection with respect to pending independent claim 8, the Office Action, at page 10, essentially asserts that the Franklin et al. patent discloses all the claimed features except for a credit card number that is deactivated upon the occurrence of a use-triggered condition. (See page 10, lines 3-22.) With respect to independent claim 16, the Office Action does not mention how the Franklin et al. patent is to be interpreted to teach or suggest a limited use credit card number which is deactivated upon a use-triggered conditions which occurs subsequent to the assignment of the a limited use credit card number. As pointed out on pages 12-13 of the Brief filed May 6, 2003, the Franklin et al. patent does not teach or suggest these features. Hence, it appears that the Office Action is relies on the Cohen patent for allegedly teaching the claimed features missing in the disclosure of the Franklin et al. patent. It is respectfully submitted, however, that this rejection based on the Cohen patent is overcome because the disclosure of the Irish priority Application No. S98 0223 filed on March 25, 1998, fully supports the subject matter set forth in independent

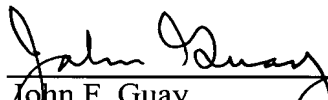claims 8 and 16. For the Examiner's convenience, a copy of the Irish priority document is attached hereto.

For instance, support for independent claims 8 and 16 can be found throughout Application No. S98 0223, for example, on page 5, lines 18-20; page 6, lines 18-19 and line 23 to page 7, line 3, page 11, lines 28-34; page 13, lines 27-35; page 14, lines 27-30; and page 15, lines 9-11. Additionally, this priority document is in the English language and predates the domestic priority date of the Cohen patent. Accordingly, it is believed that the Section 103 rejection based on the Franklin et al. and Cohen patents has been overcome.

The application is believed to be in condition for allowance, and prompt notice of same is earnestly solicited.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: _____
John F. Guay
Registration No. 47,248

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: April 6, 2004

- 1 -

"Improvements in and relating to Credit Cards"

Introduction

The present invention relates to credit card use and in particular to remote credit card use i.e. where the credit card is not necessarily physically used in the
5   transaction, but is not limited to such remote credit card use.

In this specification the term "master credit card number" refers to the credit card number as generally understood i.e. that allocated by the credit card
10   provider and generally embossed on the card and "credit card number" or "generated secure credit card" means a different credit card number as generated or provided in accordance with the invention as will be described below.

15   The development of retail electronic commerce has been relatively slow in spite of the perceived demand for such trade. The single greatest deterrent for the expansion of retail electronic commerce is the potential for fraud. This potential for fraud has been a major
20   concern for the credit card companies and financial institutions as well as the customers.

The former are seriously concerned about fraud, because essentially in the long run the financial institutions have to bear the cost of the fraud. Additionally the
25   credit card companies have a very efficient credit card system which is working extremely well for face to face transactions, i.e. transactions where the credit card is physically presented to a trader and the trader can obtain the master credit card number, compare signatures
30   and in many cases photographs before accepting a particular credit card.

The latter are equally concerned about fraud, being well aware that ultimately the user must pay for the service. However, there are particular personal concerns for the
35   consumer in that the fraudulent use of the credit card

by misuse of the master credit card number by a third party may not become apparent for some time. This can happen even if the card is still in his or her possession. Further when fraud does occur the consumer has the task of persuading the credit card provider that fraud did indeed occur.

There is also the additional fear of being overcharged on a credit card. There are thus particular risks for those credit card holders who have relatively high spending limits, in that if fraud should occur, it may be some considerable time before it is detected.

For remote credit card use, the credit card holder has to provide details of name, master credit card number, expiry date and address and often many other pieces of information for verification. This of itself is a considerable security risk as anybody will appreciate that this information could be used to charge goods and services to the card holder's credit card account. Such fraudulent use is not limited to those people to whom the credit card information has been given legitimately, anybody who can illegitimately obtain such details can conduct such fraud. A major problem in relation to this form of fraud is that the credit card may still be in the possession of the legitimate holder as these fraudulent transactions are taking place. This is often referred to as "compromised numbers" fraud. Indeed all this fraud needs is one dishonest staff member for example in a shop, hotel or restaurant to record the credit card number. It is thus not the same as card theft.

Many solutions have been proposed to this problem, however none of them allow the use of existing credit cards. Ideally the solution would be to obtain the functionality of a credit card, while never in fact revealing the master credit card number. Unfortunately, the only way to ensure that master credit card numbers cannot be used fraudulently is to never transmit the master credit card number by any direct route i.e. phone, mail, Internet or even or to print out the master

credit card number during a transaction such as is commonly the case at present. It is thus impossible.

The current approaches to the limiting of credit card fraud are dependent firstly on the theft of a card being reported and secondly elaborate verification systems whereby altered patterns of use initiate some enquiry from the credit card company. All users of credit cards have no doubt received telephone calls, when their use of the card has been exceptional, or otherwise unusual.

Thus, there have been many developments in an effort to overcome this fundamental problem of fraud, firstly in the general area of fraud for ordinary use of credit cards and then for the particular problems associated with such remote use.

One of the developments has been the provision of smart cards which are credit card devices containing embedded electronic circuitry that can either store information or perform computations. Generally speaking they contribute to credit card security systems by using some encryption system.

Another method used is the Secure Electronic Transaction (SET) protocol which represents the collaboration between many leading computer companies and the credit card industry which is particularly related to electronic transmission of credit card details and in particular via the Internet. It provides a detailed protocol for encryption of credit card details and verification of participants in an electronic transaction.

There are then specific electronic transaction systems such as "Cyber Cash", "Check Free" and "First Virtual". Unfortunately, there are serious problems with what has been proposed to date. Firstly, any form of reliance on encryption is a challenge to those who will then try to break it. The manner in which access has been gained to extremely sensitive information in Government premises, would make even the most foolhardy wary of any reliance

on an encryption system. A further problem is that some
of the most secure forms of encryption system are not
widely available due to government and other security
requirements. Limiting the electronic trading systems
and security systems for use to the Internet is of
relatively little use. While it is perceived to be an
area of high risk, in practice to date it is not.

One of the problems with all these systems is that there
are many competing technologies and therefore there is a
multiplicity of incompatible formats which will be a
deterrent to both traders and consumers. Similarly,
many of these systems require modifications of the
technology used at the point of sale, which will require
considerable investment and further limit the uptake of
the systems.

In simple terms what is required is a much more secure
way of using existing credit cards which will not
require any modification except minor ones to existing
credit cards, nor will it require the use of expensive
or specialised equipment and thus a considerable capital
investment and thus any such system must allow its use
over a wide range of different credit cards.

The present invention is directed towards providing an
improved way of using existing credit cards and in
particular an improved way of using existing credit
cards for remote credit card transactions.

Statements of Invention

The invention comprises software and devices for the
creation of secure credit cards by exploiting the
characteristic of numerical redundancy inherent in the
composition of existing credit cards and the improvement
of present credit card systems. According to the
invention there is provided a credit card system
comprising:

        means for generating and allocating secure credit
        card numbers to a credit card account;

means for providing customer access to secure credit card numbers allocated; and

means for the clearance of secure credit cards used in transactions by credit card users.

5   Such means can incorporate software and/or devices.

The credit card account may be a new or existing account. As well as credit card numbers actual additional credit cards may be issued.

The core feature of the present invention is the
10   automatic generation of single or multiple use credit card numbers or what are effectively disposable credit card numbers.

Ideally these credit card numbers are for one single use.

15   For example, when the credit card numbers are single use credit card numbers, once processed by the merchant and communicated to the credit card company, these individual or single use credit card numbers are identified by the Credit Card company's computer system
20   in the normal fashion. The number is then deactivated and no further use can be made of that number.

In relation to the actual supply of the credit card numbers, it should be appreciated that this will not cause any difficulties to the credit card provider. For
25   example, with a standard master credit card number there are up to sixteen digits, the first of which is used to identify the credit card provider whether it be American Express, VISA, Mastercard, etc. For major banks three digits are used to identify the issuing bank. The last
30   digit in the sixteen digit master credit card number is a checksum used to confirm that the number is a valid number. This leaves a total of up to 11 digits for the account identifying number and the expiry date. Obviously for single use numbers the expiry date is
35   virtually irrelevant. Thus, using the month code of the

expiry date there are 12×10^{11} i.e. 1.2×10^{12} 1,200 billion possible unique codes available for any given credit card provider. This would allow for 50 transactions a month for 10 years for 200 million account holders, before any codes would have to be recycled or a new header code introduced. When it is understood that there are then another 10^{4} header numbers that a credit card provider can use, it will be appreciated that the structure and arrangement of existing master credit card numbers is sufficient to operate this invention with the advantage that the existing infrastructure of dealing with credit card transactions can be used with minimum modification. All that is required for the credit card provider is to store the generated numbers against the master credit card number.

Credit card numbers generated in this way are inherently highly secure because (a) they can only be used for the agreed transaction after which they are invalidated and (b) the master credit card number is never revealed to a third party. In addition such a secure credit card provides great additional flexibility in that it provides considerable consumer control over use of the card in that actions can be predetermined to meet specific requirements of individual transactions.

Such predetermined actions could be the value of the particular transaction exceeding a certain amount, the value of a number of transactions exceeding an aggregate sum, the number of uses of that credit card number, the nature or class of use of that credit card number and so on. In many instances one use of the card will ideally cause the card to be deactivated. Similarly, it is envisaged that means for deactivating the generated credit card number in response to a predetermined action may actually be linked to a specific credit card number. Thus, one credit card number could be deactivated if an attempt was made to use it for a transaction greater than one amount, while another generated secure credit card number might only be deactivated when the total number of transactions on the card exceeded for example

five. Other credit card numbers could have defined predesignated use such as for example payment of hotel or other specific bills.

Specific Description

5 Essentially there is provided systems for the provision of secure credit cards comprising three principal elements:

Element 1: Means of generating secure credit cards

It is envisaged that the credit card company would
10 allocate a new credit card prefix for secure credit card numbers. Each customer using the proposed system is allocated a subset of numbers selected from the maximal possible range of numbers for the new prefix. These new secure numbers are not linked to the master credit card
15 number by encryption or other mathematical means. The mapping of secure credit card numbers to a given master credit card is generated by a random, pseudo-random or algorithmic process generated in the software, whereby a secure credit card number for a given account holder
20 cannot be computationally derived from examination of previously used secure credit cards.

To maximise the possible number of account holders, the size of the allocation for a given account can be tailored in the software to the historical or
25 anticipated number of credit card transactions. In order to limit the number of valid secure credit cards in simultaneous circulation it is anticipated that at any given time, each account holder has only sufficient allocated secure credit card numbers to meet
30 requirements over the next defined period. The software can automatically or by operator adjustment allocate a number of secure credit cards appropriate to the usage pattern of individual customers.

Element 2: Means of providing consumer access to secure credit cards

It is envisaged according to the invention that means for providing access to the generated credit card numbers could be a smart card containing encrypted versions of credit card codes, a computer program, automatic telling machine generating a disposable single use card, automatic telling machines dispensing a generated credit card number and so on.

In describing any method of providing such credit card numbers it will be appreciated that they are effectively unlimited. The number of devices that can generate or dispense such generated credit card numbers is almost limitless.

For example, a smart card, namely a small computerised device capable of storing digital information with or without a display may be issued by the credit card company which would contain encrypted versions of the generated credit card codes. Entry of a password allows the option to release one of the codes, which is then given a use. This code could be used over the Internet, the telephone, mail order or indeed for face to face transactions. The specific credit card number can be transcribed or read electronically directly from the smart card. The advantage of this is that the user himself or herself will dispense the credit card number each time. The smart card would be loaded with a specific number of credit card numbers and additional numbers would be loaded into the card as needed.

An alternative method for use in secure transactions is to provide a computer program issued by the credit card provider. This program is issued and delivered with the codes encrypted and on activation of a password separately delivered as happens at the present moment with credit cards. This program will provide the user with a secure credit card number on demand, following activation by a secure means as described below. Such a

program offers the user a plurality of generated credit card numbers that can be used as required for such remote transactions.

Such a program could be used to generate secure credit card numbers for any remote credit card transaction such as a telephone order, mail order purchase or electronic purchase via the Internet. Specifically for Internet trade the program could interface with existing web browsers to offer a semi-automated form of electronic trade. Of particular importance is the fact that since secure credit cards follow the same numerical structure as normal credit cards, secure credit cards can be used with any existing or proposed electronic trading system (e.g. SET protocol based systems) that can use conventional credit cards. The compatibility of secure credit cards with existing electronic security systems provides a significant additional level of security and flexibility to such systems.

Various security measures are envisaged such as the provision of an activating password for the user and other security measures such as, for example, that once installed, the program cannot be copied and reinstalled on another machine by application of systems used for software protection. In this embodiment of the invention the user specifies a personal password after the original activating password has been used, which is stored using one-way encryption in the manner of UNIX passwords. The credit card numbers are encrypted using an algorithm that is dependent on the user's own defined password.

In one embodiment of the invention, this is done by specifying an interacting pattern of bit swopping of the codes based on the bit sequence of the password. Pattern masking may be used.

In this particular embodiment of the invention, every program with its own password employs a different algorithm for encryption. In use, when the password is

entered a new code is generated then deleted or marked as used.

When the credit card number is generated, the credit card number can then be used for the remote transaction.

5 In another embodiment of the invention, there is provided a physical device that must be present for the computer program to be activated. This could take the form of an encapsulated device that attaches to the computer such as a "dongle", as currently used for
10 software protection. Another such embodiment would be a card reading device which can be attached to the computer, capable of reading information from the credit card, generally off the magnetic strip attached to such credit cards. The program can only be activated in the
15 physical presence of the credit card and then with the appropriate password. This has two major advantages, firstly for the user in that even if the program were to be broken, it would still be inactive unless the actual credit card is physically present. This also has the
20 advantage for the supplier of the services in that he or she knows that a customer engaging in remote credit card was in possession of the master credit card to which the secure credit card number was linked. With such a device the master credit card is merely an activating device
25 and the master credit number is not transmitted in any form.

Another means envisaged for carrying out the invention is by use of the automated telling machines (ATMs) which are used readily. They are now available in most
30 countries in many locations. These at the present moment are used to dispense cash. It is envisaged that as well as dispensing cash and performing certain other banking transactions, that the ATMs could print out a generated credit card number for a user.

35 Further it is envisaged that the ATM would produce a disposable card providing a single use credit card. It is envisaged that these disposable credit cards would be produced from any suitable materials such as cardboard

and could carry the numeric information in the form of a magnetic strip having machine readable information to allow clearance to existing magnetic card readers at the point of sale.

5 Additionally, it is envisaged that instead of the single use or disposable credit card having a number printed thereon, the number can only be activated by use in a magnetic card reader and by the insertion by the user of a pin number. Thus, when the consumer is in possession 10 of a magnetic card reader he or she can store at home a number of disposable credit cards and use them for remote or face to face transactions as required. However, for face to face transactions the credit card user would have to insert the pin number into the credit 15 card reader.

As an additional verification step in face to face transactions the credit card user's signature can be compared against the signature on a master credit card. Thus, when stored separate from the main or master 20 credit card, these disposable credit cards can then be of limited use for face to face transactions. Further they can be limited to specific amounts of money or specific purpose and indeed have the advantage for the consumer that they are not debited to an account until 25 the actual transaction is carried out.

Element 3: Means of providing for the clearance of secure credit cards

It is envisaged that secure credit cards would be processed by merchants in the same manner as existing 30 credit cards with the merchant obtaining validation of the credit card number from the credit card company or authorised third party. The specific prefix used for secure credit cards would allow such numbers to be passed onto the appropriate clearing system. A new 35 software system or special addition to the existing system would match the secure credit card number to the master credit card account and debit the account accordingly. Merchant reimbursement following

verification of a secure credit card transaction would be performed by existing means.

The existence of multiple secure credit cards for a single master credit card account allows additional controls and limits to be placed by the use of the software on certain groups of secure credit card numbers. Such additional limits on specific secure credit card numbers would be allocated by prior arrangement between the credit card company and the account holder. Software in the secure credit card clearing system would process these additional controls in addition to the normal verification procedures used at present for credit cards.

To prevent an unnecessarily large number of valid credit card codes being active at any one time, it is envisaged that secure credit card numbers are activated sequentially but not in numerical order as previous numbers are used. In the case of secure credit card numbers issued shortly before use (e.g. by automated telling machines), such numbers could be activated at the time of issuing to the account holder.

It will be appreciated that there are major advantages of such disposable credit cards over existing credit cards in that once used, they are of no use to third parties.

A well known type of fraud, so called skimming, which involves swiping a card through a machine to record the data on the card is now eliminated. Duplication of cards becomes a thing of the past with single use cards.

It will be appreciated that a major advantage of the present invention is that it requires almost no infrastructural development, but it will allow the use of existing facilities with relatively little modification. Compared in cost with establishment of complex electronic transaction systems, secure protocols, new clearance systems and associated customer

marketing, the financial savings resulting from the invention are very considerable.

It will be appreciated that the present invention virtually eliminates the possibility of fraud and would consequently result in immediate customer acceptance.

By offering consumers the ability to engage in remote trade, it is envisaged that trading over the Internet and such other remote methods of trade will greatly increase.

The advantage of ensuring that the specific credit card account details are never disclosed to any third party is exceedingly advantageous.

The advantage in relation to personal security with this system is that the only parties who need to know the actual credit card number are the card holder and credit card company. This means that information in relation to a credit card holder cannot be obtained by illicit means. This can be important indeed beyond the realms of the actual credit card use itself, since the provision of names and address to traders in foreign countries is often a way of indicating to that trader in a foreign country that the particular residence of the person providing the credit card could then be vacant.

As far as the merchant is concerned since they are never in possession of the number of the credit card, they have no responsibility for security to the credit card user. At the same time, the merchant or trader can clear the credit card number whether it be a single use or a multiple use number, but will more likely be a single use number under the existing systems, since depending on the system used, the number has exactly the same format as a normal credit card. Further in general there are no specific modifications required to the manner in which the merchant normally processes a credit card, with the exception that where disposable cards are used an imprint cannot be taken except electronically.

In respect of the credit card company there is obviously no great difficulty in providing the additional credit card numbers.

It is envisaged that a specific header sequence for single use numbers would be provided so that the number can be recognised easily by the computer system involved in checking the validity of a given credit card number. One of the great advantages for the credit card provider is that they can modify credit card limits and so on against the credit card numbers without difficulty.

In summary, the present invention has major advantages. Primarily the invention offers a high level of security for credit card payments minimising the risk of fraudulent misuse of credit card information, whether it be for specific credit card fraud or other forms of fraud or theft. Significantly, theft of a credit card could be rendered meaningless as the master credit card number could simply be deactivated for purchases where the holder chooses to use single use cards as the normal mode of transaction.

Additionally the present invention allows existing credit cards to be used more widely and for additional purposes and implementation can be achieved with minimal modification. Depending on the particular format the invention takes, the existing credit card users may or may not need to be issued with one of the devices to produce single use credit card numbers. The credit card clearing system in the particular credit card provider only requires the storing of generated secure numbers against an account for verification and debiting.

Essentially there are no great changes required for traders or merchants, who can process the credit card numbers according to the present invention by existing systems. Thus, the invention can be readily implemented by providers of goods and services, who at the present moment wish to use credit card facilities. This latter point is of considerable advantage to the credit card providers in that there is no need for a campaign to

recruit traders and merchants to use the present invention, since the present invention can be readily used with existing equipment.

It will also be appreciated that security does not depend on encryption since as has been mentioned already, there is no such thing as a totally secure encryption system.

The present invention is particularly advantageous in that it can be applied to any form of credit card transaction whether it be physical face to face or remote transactions.

Another advantage of the present invention is that the system allows for additional controls to be placed on credit card transactions. These can be placed not just simply as in the present moment by the credit card provider, but can be also placed by the credit card user. Thus, a specific spending limit or purpose can be provided against specific credit card numbers.

The facility to predefine specific use for generated credit cards would have considerable advantage in that, for example, corporate users could limit the function of the generated cards to usage that could reasonably be related to their business. In domestic circumstances this facility would also have significant advantage.

It is envisaged that the present invention will increase the use of electronic trade and provide a further penetration of the use of credit cards into all forms of trade.

The invention is not limited to the embodiments hereinbefore described which may be varied in both construction and detail.

CRUICKSHANK & CO.